IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Jakubik et al.**	§	
	§	Group Art Unit: **2142**
Serial No. **10/615,438**	§	
	§	Examiner: **Frink, John Moore**
Filed: **July 8, 2003**	§	
	§	
For: **Technique of Detecting Denial of Service Attacks**	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

36736
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on September 11, 2007.

A fee of $510.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0461. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees, which may be required to IBM Corporation Deposit Account No. 09-0461. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0461.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation of Armonk, New York.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-10

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: None
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1-10
4. Claims allowed: None
5. Claims rejected: 1-10
6. Claims objected to: None

C. CLAIMS ON APPEAL

The claims on appeal are: 1-10

STATUS OF AMENDMENTS

No amendments were submitted after the Final Office Action of August 13, 2007.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

The subject matter of claim 1 is directed to a method of detecting a denial of service attack at a network server. The method includes counting a number of inbound packets and a number of discarded packets in a specified interval (Specification page 2, paragraph 3, pages 3-4, paragraph 8, and Figure 1, steps 102, 104, and 110). The method, responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculates a percentage of discarded packets (Specification pages 2-3, paragraph 5, pages 3-4, paragraph 8, and Figure 1, steps 110, 112, and 116). The percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. (Specification page 4, paragraph 10, and Figure 1, step 116). The method, responsive to the percentage of discarded packets exceeding a specified threshold, sets a denial of service event marker (Specification page 4, paragraph 10, and Figure 1, steps 114 and 118).

B. CLAIM 4 - DEPENDENT

Claim 4 is directed to the method of claim 3, further including resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum (Specification page 5, paragraph 11, and Figure 1, step 122).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to review on appeal are as follows:

A. GROUND OF REJECTION 1 (Claims 1-3)

Whether the Examiner failed to state a *prima facie* obviousness rejection against claims 1-3 under 35 U.S.C. §103(a) over *Krumel*, Methods and Systems Using PLD-Based Network Communication Protocols, U.S. Patent Application Publication No. 2002/0083331, June 27, 2002 (hereinafter "*Krumel*") in view of *Mimura et al.*, Method of Monitoring Quality of Communication for Each Flow, U.S. Patent No. 6,847,613, January 25, 2005 (hereinafter "*Mimura*") further in view of *Aoki et al.*, Apparatus for and Method of Measuring Communication Performance, U.S. Patent No. 6,757,255, June 29, 2004 (hereinafter "*Aoki*") and further in view of *March et al.*, Protecting a Network from Unauthorized Access, U.S. Patent Application Publication No. 2003/0043740, *March* 6, 2003 (hereinafter "*March*").

B. GROUND OF REJECTION 2 (Claims 4-10)

Whether the Examiner failed to state a *prima facie* obviousness rejection against claims 1-3 under 35 U.S.C. §103(a) over *Krumel* in view of *Mimura* further in view of *Aoki* further in view of *March* and further in view of *Rabe et al.*, Storage Area Network (SAN) Management System for Discovering SAN Components Using a SAN Management Server, U.S. Patent No. 7,194,538, *March* 20, 2007 (hereinafter "*Rabe*").

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-3)

The first ground of rejection is whether the Examiner failed to state a *prima facie* obviousness rejection against claims 1-3 under 35 U.S.C. §103(a) over *Krumel* in view of *Mimura* further in view of *Aoki* and further in view of *March*.

Claim 1 is a representative claim in this grouping of claims. Claim 1 is as follows:

> 1. A method of detecting a denial of service attack at a network server, comprising:
>
> counting a number of inbound packets and a number of discarded packets in a specified interval,
>
> responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, and
>
> responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker.

Regarding claim 1, the Examiner states that:

> Regarding claim 1, *Krumel* shows a method of detecting a denial of service attack at a network server (Fig. 18), including being responsive to the number of packets in a specified interval exceeding a specified minimum [0009-0011, 0071 -0073, 0082-00841, and setting a denial of service event marker ([0108-0109]).
>
> *Krumel* does not show counting the number of inbound packets and a number of discarded packets in a specified interval.
>
> *Mimura* shows counting the number of inbound packets and a number of discarded packets in a specified interval (col. 7 lines 1 - 16).
>
> It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of *Krumel* with that of *Mimura* in order to enable collecting and thus displaying more information about current system conditions to users, allowing said users to make more informed decisions.
>
> *Krumel* in view of *Mimura* do not show calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, as a response to the number of discarded packets.
>
> *Aoki* shows calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets (Fig. 10, col. 9 line 12 - col. 10 line 19).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of *Krumel* in view of *Mimura* with that of *Aoki* in order to express system information related to packet drops in both rates (as shown by *Krumel*) and percentages, as the are two inherently related, thus enabling providing information to users in a variety of forms.

Krumel in view of *Mimura* and *Aoki* do show being responsive to a number of discarded packets, but they do not show where this response is performing a calculation determining a percentage of discarded packets.

The examiner takes official notice that it was notoriously old and well known in the art at the time of the invention that performing an addition step (inherently involved in the tracking of said number of discarded packets) is simpler logically and computationally than calculating a percentage, which requires more complex multiplication/division.

The claimed 'responsive to a number of packets' inherently involves a simple addition step, as tracking the count of a number of items on a computer inherently utilizes addition. By performing said 'calculating a percentage' responsive to the number of discarded packets, inherently tracked by addition, the simple addition step is performed frequently (each time a packet is discarded) and the complex percentage step is performed rarely (only after a certain number of discards have occurred).

It would have been obvious to one of ordinary skill in the art at the time of the invention to perform said simple arithmetic procedure frequently and said percentage calculating procedure rarely, as that would have the predictable result of lowering processor utilization, thus increasing performance.

It thus would have been obvious to one of ordinary skill in the art at the time of the invention to perform said calculation of a percentage of discarded packets as a response to the number of discarded packets.

Krumel in view of *Mimura* and *Aoki* show setting a denial of service marker (*Krumel*, Fig. 18), but do not show where it is set responsive to the percentage of discarded packets exceeding a specified threshold.

March shows responsive to the percentage of packets exceeding a threshold, a denial of service attack is reported ([97-1031).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of *Krumel* in view of *Mimura* and *Aoki* with that of *March* in order to accurately report the occurrence of denial of service attacks.

Final Office Action dated August 13, 2007, pp. 2-4.

Appellants first respond to the rejection by showing that the proposed combination of the cited references do not teach or suggest all of the features of claim 1. Appellants will then show that no proper reason exists to combine the references to achieve the invention of claim 1.

A.1. *Krumel, Mimura, Aoki*, and *March* do not teach or suggest all of the features of claim 1

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *KSR Int'l. Co. v. Teleflex, Inc.*, No. 04-1350 (U.S. Apr. 30, 2007) (citing *In re Kahn*, 441 F.3d 977, 988 (CA Fed. 2006)). Additionally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Royka,* 490 F.2d 981, 180 USPQ 580 (CCPA 1974).

The Examiner failed to state a *prima facie* obviousness rejection against claim 1 because *Krumel, Mimura, Aoki,* and *March* do not teach or suggest all of the features of claim 1. Specifically, *Krumel, Mimura, Aoki*, and *March* fail to teach or suggest (1) the feature of "responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker," and (2) the feature of "responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets."

A.1.i. *Krumel, Mimura, Aoki*, and *March* fail to teach or suggest the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker

Krumel, Mimura, Aoki, and *March* fail to teach or suggest the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker. The Examiner asserts otherwise, citing the following portion of *March*:

> [0097] Referring to FIG. 7, the media portal 44 or 45 also includes a denial-of-service (DOS) module 600, which detects for malicious attacks from an external network (e.g., the public network 14) through the use of an algorithm that is based on media session information to establish expected traffic patterns/thresholds on a per-session basis. The media session information and expected traffic thresholds are kept in a DOS profile 602 in the storage 132 of the media portal 44 or 45. Each call session is associated with a DOS profile 602.
>
> [0098] The DOS profile 602 for RTP media packets contains codec type and frame size information for the respective call session. For voice call sessions, an audio codec in each terminal encodes audio signals

originating from an audio input device (e.g., microphone) for transmission and decodes received audio data for output to an output device (e.g., a speaker). The codec can be implemented in software or hardware. Several types of codecs are available that have varying levels of data compression and data transfer rate requirements. For example, the G.711 codec provides uncompressed communications of voice data, but has a data transfer rate requirement of 64 kbps (kilobits per second) in each direction. Other codecs, such as the G.728, G.729A, G.729, G.723.1, and G.722 have varying compression algorithms and data transfer rate requirements (which are lower than that of the G.711 codec). The listed G series of audio codecs are recommendations from the International Telecommunication Union (ITU). For communications involving video, video codecs can be used.

[0099] A frame size refers to the duration of a speech sample. For example, the frame size may be 10 milliseconds (ms), which indicates that a 10-ms sample of speech is contained in the frame. Examples of other frame sizes include 20 ms, 40 ms, and so forth. Each type of codec can support certain frame sizes. Thus, if the frame size used in a call session is 20 ms, then a terminal collects a 20-ms sample of speech and encapsulates them in a packet for transmission.

[0100] The DOS module 600 counts (at 610) the number of packets received from an external network (e.g., public network 14) in a call session during a predefined time period, which is defined by a timer 604 (which can be implemented in the media portal 44 or 45 as software, hardware, or a combination of both). The number of packets received in a predefined time period defines the rate of incoming packets. The DOS module 600 checks (at 612) the rate against a threshold in the DOS profile 602 for the call session.

[0101] For example, for RTP media, if the frame size is 20 ms, then it is expected that the incoming rate of packets should be about 50 packets per second (1 packet.div.20 ms). If the incoming rate exceeds the 50 packets per second rate by some predefined percentage (the threshold rate) for some period of time (which can also be predefined), then an attack may be occurring.

[0102] Another check performed by the DOS module 600 is to determine (at 613) the codec type specified in each media packet. For example, the RTP header information contains an identifier of the type of codec used to encode the payload data. If the codec type specified in a predetermined number of packets does not match the negotiated codec type stored in the DOS profile, then an unauthorized attack may be occurring. The format of the RTP payload (including the codec type) is specified by a "PT" (payload type) field in the RTP header. More generally, checking for the codec type

> used in incoming packets is an example of protocol-specific pattern checking of each incoming packet.
>
> [0103] If the DOS module 600 determines (at 614) that the threshold rate is exceeded, or that the validation performed at 613 failed, the DOS module 600 generates (at 616) an alarm. The alarm can be communicated to an administrator, for example. Alternatively, or additionally, the DOS module 600 can also shut down the external address and port of the media portal 44 or 45 allocated for the call session, so that further inflow of external packets in the affected call session is prevented.

March, paragraphs 97-103.

Neither the cited portion nor any other portion of *March* teaches or suggests the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker. *March* discloses a system for protecting a network from unauthorized access. In particular, *March*'s system includes a controller that is adapted to deny further entry of data units from an external network in a communications session in response to the controller detecting that a rate of incoming data units exceeds a threshold or the incoming data units do not match the pattern. The cited portion discloses checking the rate of incoming packets against a threshold. However, the rate of incoming packets is not the same as the percentage of discarded packets, as claimed.

On the other hand, claim 1 recites the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker. The cited portion differs from the claimed feature because the cited portion fails to teach or suggest the percentage of discarded packets, as defined by claim 1. In particular, claim 1 defines the feature of the percentage of discarded packets in the feature "wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets." However, the "rate of incoming packets," as disclosed in *March*, has nothing to do with the number of discarded packets. Instead, *March* discloses, "[t]he number of packets received in a predefined time period defines the rate of incoming packets." *March*, paragraph 100. Thus, as described by *March*, the rate of incoming packets is the number of packets received in a predefined time period, and does not relate to the number of discarded packets, let alone equal the number of discarded packets divided by the number of inbound packets, as claimed.

Because *March* fails to teach or suggest the feature of a percentage of discarded packets, *March* also fails to teach or suggest that anything is responsive to the percentage of discarded

packets exceeding a specified threshold, let alone the setting of a denial of service event marker, as claimed. Therefore, neither the cited portion nor any other portion of *March* teaches or suggests the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker.

Krumel, *Mimura*, and *Aoki* fail to cure the deficiencies of *March*. The Examiner admits that "*Krumel* in view of *Mimura* and *Aoki* show setting a denial of service marker (*Krumel*, Fig. 18), but do not show where it is set responsive to the percentage of discarded packets exceeding a specified threshold." Final Office Action dated August 13, 2007, p. 4. Additionally, *Krumel*, *Mimura*, and *Aoki* do not teach, suggest, or give any incentive to make the needed changes to reach claim 1. Absent the Examiner pointing out some teaching or incentive to implement *Krumel*, *Mimura*, and *Aoki* and the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker, one of ordinary skill in the art would not be led to modify *Krumel*, *Mimura*, or *Aoki* to reach the present invention when the reference is examined as a whole.

Therefore, *Krumel*, *Mimura*, *Aoki*, and *March* fail to teach or suggest the claimed feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker. Accordingly, the proposed combination of *Krumel*, *Mimura*, *Aoki*, and *March*, when considered as a whole, does not teach or suggest all of the features of claim 1. Therefore, under the standards of *In re Lowry* and *In re Grabiak*, the Examiner failed to state a *prima facie* obviousness rejection of claim 1 or any other claim in this grouping of claims.

A.1.ii. *Krumel*, *Mimura*, *Aoki*, and *March* fail to teach or suggest the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets

Krumel, *Mimura*, *Aoki*, and *March* fail to teach or suggest the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets. The Examiner asserts otherwise, citing the following portions of *March*:

FIG.10

24

NAME OF SESSION	(A, B)
ADDRESS OF TRANSMITTING-SIDE COMMUNICATIONS DEVICE	13. 204. 301. 562
ADDRESS OF RECEIVING-SIDE COMMUNICATIONS DEVICE	20. 213. 223. 442
SESSIONS START TIME	16:48:06.166396
SESSION END TIME	16:48:08.236911
TOTAL NUMBER OF PACKETS	604
TOTAL DATA QUANTITY	819202 BYTES
MAXIMUM SEGMENT SIZE	1460 BYTES
ROUND TRIP TIME	12msec
PACKET DISCARD RATE	0. 19
PACKET DISCARD EVENT RATE	0. 08

Aoki, Figure 10.

That is to say, the performance index detecting unit 22 detects a packet discard rate or a packet discard event rate instead of the average congestion window size, and set it as a performance index for calculating the effective bandwidth. When the packets are transmitted through the TCP communications, sequence numbers are imparted to the packets in order, and recorded in headers of the packets. When tracing the sequence numbers of the TCP packets per session, if the sequence number increases in order, it can be recognized that the packets are transmitted or received without being discarded. If the sequence number is reversed, the packet with this reversed number, and hence it can be known that the packet has been retransmitted. Accordingly, as shown in FIG. 8, an occurrence of the reverse of the sequence number is counted as a packet discard event, and the number of the retransmitted packets after the sequence number has been reversed, is counted as a packet discard.

A method of counting the number of the packet discards and the number of the packet discard events will be explained with reference to FIG. 9. The performance index detecting unit 22 has a memory for storing, as variables, respective values of LOSS-NUM (a packet discard counter), LOSS-EVENT-NUM (a packet discard event counter), LOSS-EVENT-FLAG (a packet discard event hysteresis flag), MAX-SEQ-NO (a maximum sequence number) and LAST-SEQ-NO (a latest transmission packet sequence number).

The performance index detecting unit 22 initializes to "0" the respective values of LOSS-NU, LOSS-EVENT-NUM, LOSS-EVENT-FLAG, and MAX-SEQ-NO. In step S2, it is detected from the log information of the packet whether or not a new packet is transmitted. When the new packet has been transmitted, the processing proceeds to step S3. Whereas if not, the process in step S2 is repeated. In step S3, a sequence number of the new packet transmitted is detected from the log information, and is substituted into LAS-SEQ-NO. The performance index detecting unit 22 checks in step S4 an establishment of such a condition that LAS-SEQ-NO is under MAX-SEQ-NO. The establishment of the condition in step S4 implies that the packet has been discarded. When the condition is established in step S4, the processing proceeds to step S5, wherein LOSS-NUM is incremented by "1". The processing advances to step S6. It is checked in step S6 whether or not LOSS-EVENT-FLAG is "1". If LOSS-EVENT-FLAG is "1", the packet discard events are already counted, and hence the processing goes back to step S2. If LOSS-EVENT-FLAG is "0", the packet discard events are not yet counted, and therefore the processing advances to step S7, in which LOSS-EVENT-NUM is incremented by "1".

If the condition is not established in step S4, the sequence number is not reversed, and the packet discard does not occur. At this time, the processing proceeds to step S8, in which a value of LAST-SEQ-NO is substituted into MAX-SEQ-NO. Next, LOSS-EVENT-FLAG is reset to "0" in step S9. The processing returns to step S2. Just when the session is finished, a value of LOSS-NUM is given as the number of the packets discarded, and a value of LOSS-EVENT-NUM is given as the number of packet discard events. The performance index detecting unit 22 obtains a packet discard rate and a packet discard event rate by using these values in the way which follows.

A packet discard rate p, with the performance index detecting unit 22 detecting the number of packets (the number of packets discarded) of which the receipts are not confirmed by the receiving acknowledgement packet and a total number of packets transmitted or received by referring to the packet log information per session, is calculated in the formula (4):

p=Number of discarded packets/Total number of packets

According to the congestion avoidance algorithm of the TCP, when the packet is discarded in the window size, even if a plurality of packets might be discarded, this packet discard is conceived as one single congestion signal, and the window size is adjusted (reduced down to the half). Accordingly, the occurrence that the sequence number is reversed is conceived as one single packet discard event, and a packet discard event

> rate q is calculated by the formula (5). Note that an accuracy of estimation is more enhanced by obtaining the effective bandwidth using this event rate q.
>
> q=Number of packet discard events/Total number of packets

Aoki, column 8, line 66 – column 10, line 19.

Neither the cited portion nor any other portion of *Aoki* teaches or suggests the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets. *Aoki* discloses a system for measuring performance in TCP and UDP communications. *Aoki* discloses measuring performance using a calculated performance index, such as the 'p' and 'q' performance indices disclosed in the cited portion. However, *Aoki* nowhere teaches or suggests that the calculation of 'p' or 'q' is responsive to the number of discarded packets.

On the other hand, claim 1 recites the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets. As a first matter, the Examiner admits that "*Krumel* in view of *Mimura* and *Aoki* do show being responsive to a number of discarded packets, but they do not show where this response is performing a calculation determining a percentage of discarded packets." Final Office Action dated August 13, 2007, p. 3.

As a second matter, even assuming, *arguendo*, that the calculation of 'p' in *Aoki* teaches or suggests the percentage of discarded packets, as claimed, the cited portion still fails to teach or suggest that the calculation of 'p' has a "responsive to" relationship with the number of discarded packets, let alone with the number of discarded packets in the specified interval exceeding a specified minimum.

For example, the cited portion states that "[a] packet discard rate p, with the performance index detecting unit 22 detecting the number of packets (the number of packets discarded) of which the receipts are not confirmed by the receiving acknowledgement packet and a total number of packets transmitted or received by referring to the packet log information per session, is calculated in the formula (4)." *Aoki*, column 9, line 64 – column 10, line 3. However, the cited statement nowhere teaches or suggests any "responsive to" relationship between calculating 'p' and the number of discarded packets in a specified interval exceeding a specified minimum.

As a third matter, the Examiner incorrectly asserts official notice of the fact that "[i]t ... would have been obvious to one of ordinary skill in the art at the time of the invention to perform said calculation of a percentage of discarded packets as a response to the number of discarded packets." Final Office Action dated August 13, 2007, p. 4. In particular, the Examiner assertion of official notice fails to address the entire feature of "responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets." Instead, the Examiner addresses only whether the calculation step is responsive to "the number of discarded packets," thereby failing to take into account all features of the claim 1. Thus, the Examiner's assertion of official notice fails to demonstrate that the feature of calculating a percentage of discarded packets is responsive to the number of discarded packets in the specified interval exceeding a specified minimum, as claimed, and, as shown above, and the Examiner actually admits that "*Krumel* in view of *Mimura* and *Aoki* do show being responsive to a number of discarded packets, but they do not show where this response is performing a calculation determining a percentage of discarded packets." Final Office Action dated August 13, 2007, p. 3.

March fails to cure *Krumel*, *Mimura*, and *Aoki's* lack of disclosure. *March* discloses a system for protecting a network from unauthorized access, but nowhere teaches or suggests a percentage of discarded packets, as claimed in claim 1. Therefore, *Krumel*, *Mimura*, *Aoki*, and *March* fail to teach or suggest the claimed feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets. Accordingly, the proposed combination of *Krumel*, *Mimura*, *Aoki*, and *March*, when considered as a whole, does not teach or suggest all of the features of claim 1. Therefore, under the standards of *In re Lowry* and *In re Grabiak*, the Examiner failed to state a *prima facie* obviousness rejection of claim 1. As a consequence, no *prima facie* obviousness rejection has been stated against claims 2 and 3, at least by virtue of their dependency on claim 1.

A.2. The Examiner failed to state a sufficient reason to combine the references in light of the major differences between the reference and the claim 1

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). The scope and content of the prior art are... determined;

differences between the prior art and the claims at issue are... ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or non-obviousness of the subject matter is determined. *Graham v. John Deere Co.*, 383 U.S. 1 (1966). Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. *KSR Int'l. Co. v. Teleflex, Inc.*, No. 04-1350 (U.S. Apr. 30, 2007). Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *Id.* (citing *In re Kahn*, 441 F.3d 977, 988 (CA Fed. 2006)).

In the case at hand, no *prima facie* obviousness rejection can be stated because the Examiner failed to state a sufficient reason to combine *Krumel*, *Mimura*, *Aoki*, and *March* in light of the differences between the cited references and claim 1. Specifically, as shown in Section A.1, *Krumel*, *Mimura*, *Aoki*, and *March* fail to teach or suggest (1) the feature of "responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker", and (2) the feature of "responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets." Because *Krumel*, *Mimura*, *Aoki*, and *March* fail to teach or suggest at least these claimed features, major differences exist between the cited references and claim 1 under the *Graham v. John Deere Co.* inquiry set forth above.

Furthermore, the Examiner failed to state a sufficient reason to combine *March* with *Krumel*, *Mimura*, and *Aoki* in light of the differences that exists between the cited references and claim 1. The Examiner failed to state a sufficient reason to combine *Krumel*, *Mimura*, *Aoki*, and *March* because the Examiner's proposed reason for combining *Krumel*, *Mimura*, *Aoki*, and *March* provides no rational underpinning to support a legal conclusion of obviousness. Regarding a reason to combine *Krumel*, *Mimura*, *Aoki*, and *March*, the Examiner states that:

> It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of *Krumel* in view of *Mimura* and *Aoki* with that of *March* in order to accurately report the occurrence of denial of service attacks.

Final Office Action dated August 13, 2007, p. 4.

The Examiner offers an advantage as the stated reason for combining *Krumel*, *Mimura*, *Aoki*, and *March* in the manner proposed by the Examiner. Specifically, the Examiner proposes combining *Krumel*, *Mimura*, *Aoki*, and *March* "in order to accurately report the occurrence of denial of service attacks." However, the Examiner fails to provide a sufficient reason to combine *Krumel*, *Mimura*, *Aoki*, and *March* because *Krumel* already achieves the advantage set forth by the Examiner. Specifically, *Krumel* reports the presence and severity of attacks using visual and audio output. For example, *Krumel* provides that:

> [0116] In the preferred embodiment, parallel to server mode button 200 on the external side of the case is alert button 204, which contains alert LED 206. Alert LED 206 is coupled to alarm controller 53 (as illustrated in FIG. 3), which preferably is implemented as a part of PLD 162 (as illustrated in FIG. 9). Alert LED 206 may contain a single or multi-colored LED, which, when illuminated, indicates the data protection system is under attack and is rejecting suspect packets. The data protection system preferably registers the frequency of attacks and sends signals to alert LED 206 based on such information. In a preferred embodiment, alert LED 206 may contain a LED (e.g., red), which remains consistently illuminated during irregular attacks or blinks at regular intervals under heavy attack. In another preferred embodiment, alert LED 206 may contain a multi-colored LED, which similarly indicates when the system is under attack and is rejecting packets. With a multi-colored LED, the increase in frequency or intervals of attacks may be indicated by a change in color: for example, green (indicating no registered attacks by suspect packets) to yellow (indicating a few irregular attacks) to red (indicating more frequent attacks) to blinking red (indicating a heavy attack). The alert alarm may be reset by depressing alert button 204.
>
> [0117] In a preferred embodiment, speaker 55 (or some form of audio transducer) may be coupled to alarm controller 53 to also indicate the presence or severity of attacks (as described in connection with FIG. 3). For example, when the data protection system is under heavy attack and alert LED 206 is blinking (e.g., red), an alarm signal may be transmitted to speaker 55 to emit audio information to indicate a suspected severe attack or emergency. Alarm-type information may also be coupled to the internal network (such as via a LDP packet, as described elsewhere herein), and thus transmit alarm information over the network to a software interface on the desktop. In other embodiments of the data protection system, an array of different features, including buttons, LEDs, alarms, and graphical user interfaces, may be utilized to indicate the class, frequency and severity of attacks on the system.

Krumel, paragraphs 116 and 117.

Thus, *Krumel* already achieves the advantage offered in the Examiner's proposed reason for combining *March* with *Krumel*, *Mimura*, and *Aoki*, thereby depriving one of ordinary skill in

the art any reason to look to *March* to achieve the advantage. Because *Krumel* already achieves the advantage offered by the Examiner as a reason to combine *March* with *Krumel*, *Mimura*, and *Aoki*, the cited advantage cannot provide a rational underpinning to support a legal conclusion of obviousness. For this reason, the Examiner's reason for combining *Krumel*, *Mimura*, *Aoki*, and *March* provides insufficient basis for combining *Krumel*, *Mimura*, *Aoki*, and *March* in the manner proposed by the Examiner, especially in light of the major differences that exist between the cited references and claim 1. Accordingly, no *prima facie* obviousness rejection has been stated against claim 1.

B. GROUND OF REJECTION 2 (Claims 4-10)

The second ground of rejection is whether the Examiner failed to state a *prima facie* obviousness rejection against claims 4-10 under 35 U.S.C. §103(a) over *Krumel* in view of *Mimura* further in view of *Aoki* further in view of *March* and further in view of *Rabe*.

Claim 4 is a representative claim in this grouping of claims. Claim 4 is as follows:

> 4. The method of claim 3, wherein the flood monitoring process comprises:
>
> resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum.

Regarding claim 4, the Examiner states that:

> *Krumel* in view of *Mimura*, *Aoki* and *March* do not show resetting the denial of service event marker if a number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum.
>
> *Rabe* shows resetting an alarm after a second specified minimum (in *Rabe*'s case, specified as normal operating conditions) is reached (col. 21 lines 50 - 67).
>
> It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of *Krumel* in view of *Mimura*, *Aoki* and *March* with that of *Rabe* to prevent an alarm from sounding incessantly as well as to ensure that said alarm was only active when alarm conditions were present.
>
> *Krumel* in view of *Mimura*, *Aoki* and *March* and Reba [sic] do not explicitly show where said monitoring is done in the interval before execution of the flood monitoring process. However, *Mimura*, as described in the response to claim 2, shows monitoring at all intervals (Fig. 7) unless

> specifically shut down. It thus would have been obvious to monitor for the packet drop rate to return to normal at all times, including before execution of the flood monitoring process

Final Office Action dated August 13, 2007, pp. 5-6.

Appellants first respond to the rejection by showing that the proposed combination of the cited references do not teach or suggest all of the features of claim 4. Appellants will then show that no proper reason exists to combine the references to achieve the invention of claim 4.

B.1. *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe* do not teach or suggest all of the features of claim 4

The Examiner failed to state a *prima facie* obviousness rejection against claim 4 because *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe* do not teach or suggest all of the features of claim 4. As shown in Section A.1., *Krumel*, *Mimura*, *Aoki*, and *March* fail to teach or suggest all of the features of claim 1. Therefore, *Krumel*, *Mimura*, *Aoki*, and *March* fail to teach or suggest all of the features of claim 4, which depends from claim 1. In addition, claim 4 claims other additional combinations of features not taught or suggested by the references.

For example, *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe* fail to teach or suggest the feature of resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum. The Examiner asserts otherwise, citing the following portion of *Rabe*:

> One type of policy is a threshold condition with action policy. These policies may be used to monitor an object and detect when a particular numeric threshold is reached and sustained for a configurable period. The collector on which a threshold condition is based may provide data in numeric form, for example as numbered units or a percentage. This type of policy may also reset the alarm when the value being monitored returns to a normal, or below threshold value. Both the alarm state and the clear state of a threshold condition may be configured when defining the policy. As an example of a threshold condition with action policy, "If port utilization >90% of capacity for 1 minute, then post a critical alert to the SAN manager and send e-mail to the administrator." A threshold condition with action policy may also provide a condition to reset the alert when the value being monitored returns to a normal, or below threshold value. For example, "If port utilization <=75% for 1 minute, then clear the critical alert."

Rabe, column 21, lines 50-67.

Neither the cited portion nor any other portion of *Rabe* teaches or suggests the feature of resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum. *Rabe* discloses a storage area network management system for discovering storage area network components using a storage area network server. As a general matter, *Rabe* does not address the issue of denial of service attacks. The cited portion discloses the resetting of an alarm when a value falls below a threshold. However, the cited portion nowhere mentions a denial of service event marker.

On the other hand, claim 4 recites the feature of resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum. The cited portion differs from the claimed feature because the alarm and alert in *Rabe* is not the same as a denial of service event marker. The alarm and alert in *Rabe* does not relate to a denial of service event. For example, *Rabe* explicitly defines the alarm and alert as follows:

> An alarm is a signal that is generated by a policy when the condition specified in the policy is detected or evaluated as true. An alarm may be triggered if the condition and alarm action are configured in the policy. Note that alarms are associated with alerts, but are not the same. An alarm is an internal signal used by the SAN management system. An alert to the SAN manager 202 is a configurable responses that may result from an alarm being triggered.

Rabe, column 21, lines 13-20.

The cited portion relates alarms and alerts to a storage area network management system, but nowhere relates alarms and alerts to denial of service events. Because neither the cited portion nor any other portion of *Rabe* teaches or suggests the feature of a denial of service event marker, *Rabe* also fails to teach or suggest resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum.

Krumel, *Mimura*, *Aoki*, and *March* fail to cure *Rabe*'s lack of disclosure. The Examiner admits that "*Krumel* in view of *Mimura*, *Aoki* and *March* do not show resetting the denial of service event marker if a number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum." Final Office Action dated August 13, 2007, p. 5. Additionally, *Krumel*, *Mimura*, *Aoki*, and *March* do not teach,

suggest, or give any incentive to make the needed changes to reach claim 4. Absent the Examiner pointing out some teaching or incentive to implement *Krumel*, *Mimura*, *Aoki*, and *March* and the feature of resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum, one of ordinary skill in the art would not be led to modify *Krumel*, *Mimura*, *Aoki*, or *March* to reach the present invention when the reference is examined as a whole.

Therefore, *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe* fail to teach or suggest the claimed feature of resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum. Accordingly, the proposed combination of *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe*, when considered as a whole, does not teach or suggest all of the features of claim 4. Therefore, under the standards of *In re Lowry* and *In re Grabiak*, the Examiner failed to state a *prima facie* obviousness rejection of claim 4 or any other claim in this grouping of claims.

B.2. The Examiner failed to state a sufficient reason to combine the references in light of the major differences between the reference and claim 4

In the case at hand, no *prima facie* obviousness rejection can be stated because the Examiner failed to state a sufficient reason to combine *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe* in light of the differences between the cited references and claim 4. Specifically, as shown in Section B.1., *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe* fail to teach or suggest the feature of resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum. Because *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe* fail to teach or suggest at least this claimed feature, major differences exist between the cited references and claim 4 under the *Graham v. John Deere Co.* inquiry set forth above.

Furthermore, the Examiner failed to state a sufficient reason to combine *Rabe* with *Krumel*, *Mimura*, *Aoki*, and *March* in light of the differences that exists between the cited references and claim 4. The Examiner failed to state a sufficient reason to combine *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe* because the Examiner's proposed reason for combining *Krumel*,

Mimura, *Aoki*, *March*, and *Rabe* provides no rational underpinning to support a legal conclusion of obviousness. Regarding a reason to combine *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe*, the Examiner states that:

> It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of *Krumel* in view of *Mimura*, *Aoki* and *March* with that of *Rabe* to prevent an alarm from sounding incessantly as well as to ensure that said alarm was only active when alarm conditions were present.

Final Office Action dated August 13, 2007, p. 5.

The Examiner offers an advantage as the stated reason for combining *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe* in the manner proposed by the Examiner. Specifically, the Examiner proposes combining *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe* "to prevent an alarm from sounding incessantly as well as to ensure that said alarm was only active when alarm conditions were present." However, the Examiner fails to provide a sufficient reason to combine *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe* because *Krumel* already achieves the advantage set forth by the Examiner. Specifically, *Krumel* discloses an alert button that resets an alert alarm, as well as a particular indicator for signaling when no attack is present. For example, *Krumel* provides that:

> [0116] In the preferred embodiment, parallel to server mode button 200 on the external side of the case is alert button 204, which contains alert LED 206. Alert LED 206 is coupled to alarm controller 53 (as illustrated in FIG. 3), which preferably is implemented as a part of PLD 162 (as illustrated in FIG. 9). Alert LED 206 may contain a single or multi-colored LED, which, when illuminated, indicates the data protection system is under attack and is rejecting suspect packets. The data protection system preferably registers the frequency of attacks and sends signals to alert LED 206 based on such information. In a preferred embodiment, alert LED 206 may contain a LED (e.g., red), which remains consistently illuminated during irregular attacks or blinks at regular intervals under heavy attack. In another preferred embodiment, alert LED 206 may contain a multi-colored LED, which similarly indicates when the system is under attack and is rejecting packets. With a multi-colored LED, the increase in frequency or intervals of attacks may be indicated by a change in color: for example, green (indicating no registered attacks by suspect packets) to yellow (indicating a few irregular attacks) to red (indicating more frequent attacks) to blinking red (indicating a heavy attack). The alert alarm may be reset by depressing alert button 204.

Krumel, paragraph 116 (emphasis added).

Thus, *Krumel* already achieves the advantage offered in the Examiner's proposed reason for combining *Rabe* with *Krumel*, *Mimura*, *Aoki*, and *March*, thereby depriving one of ordinary

skill in the art any reason to look to *Rabe* to achieve the advantage. Because *Krumel* already achieves the advantage offered by the Examiner as a reason to combine *Rabe* with *Krumel*, *Mimura*, *Aoki*, and *March*, the cited advantage cannot provide a rational underpinning to support a legal conclusion of obviousness. For this reason, the Examiner's reason for combining *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe* provides insufficient basis for combining *Krumel*, *Mimura*, *Aoki*, *March*, and *Rabe* in the manner proposed by the Examiner, especially in light of the major differences that exist between the cited references and claim 4. Accordingly, no *prima facie* obviousness rejection has been stated against claim 4. As a consequence, no *prima facie* obviousness rejection has been stated against claims 5-10, at least by virtue of their dependency on claims 1 or 4, which have been shown above to be non-obviousness over the cited references.

/Gerald H. Glanzman/

Gerald H. Glanzman
Reg. No. 25,035
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Appellants

GG/ka

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method of detecting a denial of service attack at a network server, comprising:

counting a number of inbound packets and a number of discarded packets in a specified interval,

responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, and

responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker.

2. The method of claim 1, further comprising:

collecting inbound packet information to further characterize the denial of service attack.

3. The method of claim 2, wherein collecting the inbound packet information further comprises:

initiating a flood monitoring process that is executed at designated intervals to collect the inbound packet information while the denial of service attack is in progress.

4. The method of claim 3, wherein the flood monitoring process comprises:

resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum.

5. The method of claim 3, wherein the flood monitoring process comprises:

resetting the denial of service event marker if a rate of discarded packets in the specified interval before execution of the flood monitoring process is less than a second specified threshold.

6. The method of claim 4, further comprising:

collecting the inbound packet information to further characterize the denial of service attack when the denial of service attack is declared over.

7. The method of claim 6, wherein the inbound packet information includes at least one of:

a) a number of inbound packets in a last interval;

b) a number of discarded packets in a last interval;

c) a packet discard rate;

d) a most frequent discard protocol type;

e) a most frequent discard type; and

f) a media access control address of an immediately prior packet hop.

8. The method of claim 3, wherein the flood monitoring process comprises:

determining if the denial of service attack is still in progress by comparing packets discarded in a last interval with the number of inbound packets, and

maintaining the flood monitoring process if the denial of service attack is still in progress.

9. The method of claim 8, further comprising:

collecting inbound packet information for the last interval.

10. The method of claim 5, further comprising:

collecting additional inbound packet information to further characterize the denial of service attack when the denial of service attack is declared over.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.